

EXHIBIT G

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

SOUTHWEST AIRLINES CO.,

Plaintiff,

v.

KIWI.COM, INC. and KIWI.COM

S.R.O.,

Defendants.

§
§
§
§
§
§
§
§
§
§

Civil Action No. 3:21-cv-00098-E

DECLARATION OF MICHAEL ERDMAN

I, Michael Erdman, being duly sworn, state as follows:

1. My name is Michael Erdman and I am a Senior Manager for Technology at Southwest Airlines Co. (“Southwest”) with responsibility for software engineering.

2. As part of my duties, I am familiar with how Southwest hosts data and supports functionality for Southwest’s website at www.southwest.com (“Southwest.com”) and the Southwest Apps, including information relating to flight schedules, fares, and booking reservations.

3. In early February 2021, after business partners notified IT of Kiwi’s actions, we implemented technical measures to identify and monitor Kiwi’s automated access of Southwest.com.

4. Prior to February 24, 2021, our application logs and automated bot protection product showed that Kiwi was using automated web-scraping script to access the “front end” of Southwest.com and scrape data (referenced herein as “Front-End Scraping”). Kiwi’s “bots” accessed Southwest.com from the front end in the same way that an individual user does. The only

difference was that instead of physically clicking a mouse through the searching and booking process (e.g., selecting the preferred flight and clicking purchase), the bots automated the process. When the automated bot purchased a ticket, the bot sent a “request” to purchase the flight to Southwest’s HTML. The automated scripting still directly interacted with Southwest’s HTML. Even though the bot was not physically clicking the “Purchase” button with a mouse, the automated request that the bot sent to Southwest.com was the same as if an individual user had clicked “Purchase.”

5. On February 24, 2021—the same day that Southwest filed its Motion for Preliminary Injunction—Southwest implemented a security measure that blocked Kiwi’s Front-End Scraping. This was successful for a few weeks until Kiwi developed other hacks.

6. Over the next few weeks, our logs show that an individual user from Kiwi manually accessed and purchased tickets through the front end of Southwest.com. We know the individual user(s) was from Kiwi because the transactions have specific kiwi domain email addresses associated to them. We believe Kiwi was trying to reverse engineer our architecture by using these transactions. Through this method, Kiwi purchased the flights directly from the front end of Southwest.com. Kiwi’s web browser directly interacted with and sent requests to Southwest’s HTML as Kiwi proceeded through the booking process.

7. Soon after the February 24th blocking measure, Kiwi began hacking Southwest’s application programming interface or “API”¹ at <https://www.southwest.com/api/air-booking/v1/air-booking/page/air/booking/confirmation> with automated bots (referenced herein as “API Hacking”). Kiwi hacked Southwest’s API after determining the correct “request” format

¹ API is an interface used to programmatically access an application through a set of routines, protocols, and other tools for building software applications. The purpose of using an API is to access an application without using the standard user interface.

required by the API. After Kiwi identified the proper request format and a way to bypass our automated bot detection product, it attacked Southwest's API with automated scripts and continued to access, scrape, and republish Southwest data (just as it had done using Front-End Scraping)

8. On the morning of April 5, 2021, Southwest implemented another measure to block Kiwi's API Hacking. Within eight hours of implementing this second blocking measure, Kiwi developed another hack to bypass Southwest's blocking technology.

9. With each blocking measure Southwest implements, Kiwi continues to hack Southwest.com by changing the way it architects its automated scripts to access, scrape, and republish data from Southwest.com.

10. I have read the Declaration of Jozef Kèpesi, Kiwi's Chief Technology Officer. In Paragraphs 7 through 13, Kèpesi describes the process by which Kiwi is currently accessing, scraping, and republishing Southwest data. Notably, he does not deny that Kiwi is scraping and republishing the data, but argues that Kiwi's activities are permissible because Southwest has made its API "publicly available," which is not true.²

11. Kèpesi fails to acknowledge that before Southwest filed the Motion for Preliminary Injunction and implemented the February 24th blocking measure, Kiwi was using Front-End Scraping. The process he describes in his Paragraphs 7 through 13, is the API Hacking method I described above. Kiwi only began using API Hacking after we blocked Kiwi's Front-End Scraping on February 24, 2021.

12. Kèpesi also mischaracterizes the permissibility of API Hacking. Southwest has not made its API "publicly available" in the way Kiwi is currently accessing and utilizing it. An API request has to go through southwest.com for it to become publicly available and an API key is

² See Ex. A-3, Website Terms at 1-2 (App. 40-41).

required in the request. Our API's can't be accessed directly as they sit behind our firewall for protection. Further, impermissible "scraping" does not have the narrow definition that Kèpesi indicates; scraping is not merely "accessing public-facing HTML pages and parsing information out of that HTML."

13. Kèpesi admits Kiwi is scraping and hacking Southwest's API in the exact manner prohibited by the Website Terms:³

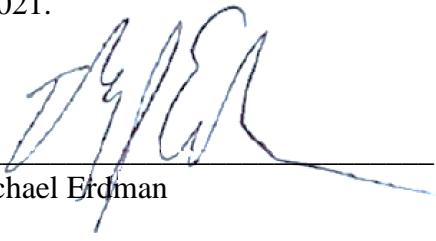
11. Kiwi.com programmatically interprets and aggregates the data from Southwest's responses, along with data similarly collected via requests to other airlines, to build itinerary options for its customers.

Kiwi's "programmatically" (i.e., automatically) interpreting, aggregating, and republishing of Southwest data—API Hacking—is the precise action Southwest seeks to enjoin.

14. Not only does Kèpesi admit Kiwi is currently utilizing API Hacking, but by attempting to distinguish Front-End Scraping from API Hacking, Kèpesi concedes that Kiwi's pre-February 24th Front-End Scraping was a violation of the Website Terms.

15. I declare under penalty of perjury that the facts and information stated in this declaration are true and correct based on my personal knowledge and reliable information I obtained as a representative of Southwest.

Executed in Dallas, Texas on April 14, 2021.


Michael Erdman

³ See Ex. A-3, Website Terms at 1-2 (App. 40-41).